JOURNAL OF ALGEBRA 60, 158–168 (1979)

Permutation Representations of the Finite Classical Groups of Small Degree or Rank

WILLIAM M. KANTOR*

University of Oregon, Eugene, Oregon 97403

Communicated by Graham Higman

Received June 15, 1978

1. INTRODUCTION

In 1832, Galois [11, pp. 411–412] determined the smallest degree of a faithful permutation representation of PSL(2, q) for q a prime; the case q a prime power was handled much later, reportedly first in unpublished work of Moore in 1894 (see Loewy [22]). The corresponding problem was solved for Sp(4, q), q an odd prime or prime power, by Dickson [9] and Mitchell [27], respectively; and for SL(3, q) and SU(3, q) by Mitchell [26] and Hartley [13]. In a beautiful but unpublished thesis written in 1972, Patton [29] proved the corresponding results for all the groups SL(n, q), as well as for Sp($2m$, q) with q odd. More recently, Cooperstein [5] used Patton's method to settle this type of question for all the remaining classical groups. The result is that the smallest degree is attained precisely when the one-point stabilizer is a suitable reducible group, with just a few sporadic exceptions.

This still leaves open the problem of how small an *irreducible* subgroup of one of the classical groups must be. The purpose of this paper is to use Patton's method to provide some answers to this question.

THEOREM 1. *Let* $\mathrm{SL}(n, q) \leqslant G \geqslant \Gamma\mathrm{L}(n, q)$ *with* $n \geqslant 3$, *and let* $K \leqslant G$. *Assume that* $|G:K| \leqslant q^{n(n-1)/2}$ *if* q *is odd and* $q > 3$ (*or that* $|G:K| \leqslant q^{(n-1)(n-2)/2}$ *if* $q > 2$, *or that* $|G:K| \leqslant q^{(n-2)(n-3)/2}$ *if* $q = 2$. *Then either* (i) K *is reducible or* (ii) $K \trianglerighteq \mathrm{SL}(n, q)$ *or* $\mathrm{Sp}(n, q)$.

For small n, this result is weaker than Patton's: he showed that if $K \not\trianglerighteq \mathrm{SL}(n, q)$, then $|G:K| \geqslant (q^n - 1)/q - 1)$, with only one exception ($K = A_7 < \mathrm{SL}(4, 2)$). For large q, the bound $q^{n(n-1)/2}$ is very roughly the index $|G:B|$ of a Borel subgroup (i.e., the number of complete flags; cf. Section 7). In the case of the remaining classical groups, our bounds are closer to $|G:B|^{1/2}$:

* This research was supported in part by Oxford University, the Science Research Council, and the National Science Foundation.

0021-8693/79/090158–11$02.00/0

THEOREM 2. *Let* $G^\natural$ *be* $\mathrm{Sp}(2m, q)$, $m \geqslant 4$, q *odd*; $\mathrm{SU}(n, q)$, $n \geqslant 4$; *or* $\Omega^{\pm}(n, q)$, $n \geqslant 5$. *Let* $G^\natural \leqslant G \leqslant \Gamma\mathrm{Sp}(2m, q)$, $\Gamma U(n, q)$, *resp.* $\Gamma O^{\pm}(n, q)$, *and let* $K \leqslant G$ *with* $K \ngeqslant G^\natural$. *Then* K *is reducible (and has a proper invariant subspace other than the radical of the underlying vector space if* $G^\natural = \Omega(2m+1, q)$, q *even) if* $|G : K| < q^\theta$ *with* θ *as follows*:

(i) $G^\natural = \mathrm{Sp}(2m, q)$, q *odd*, $\theta = \frac{1}{2}m(m+1)$;

(ii) $G^\natural = \mathrm{SU}(n, q)$, $\theta = [n^2/4]$; *or*

(iii) $G^\natural = \Omega^+(2m, q)$, $\Omega(2m+1, q)$ *or* $\Omega^-(2m+2, q)$, $\theta = \frac{1}{2}m(m-1)$ *(but* $\theta = \frac{1}{2}(m-1)(m-2)$ *if* $q = 3$ *or if* $q > 2$ *and* q *is even; and* $\theta = \frac{1}{2}(m-2)(m-3)$ *if* $q = 2$*).*

As an elementary application of these theorems, we prove the following result. (Recall that the rank of a permutation representation is the number of double cosets of the one-point stabilizer.)

THEOREM 3. *Let* $G^\natural$ *be* $\mathrm{SL}(n, q)$, $\mathrm{Sp}(n, q)$ *with* q *odd*, $\mathrm{SU}(n, q)$ *or* $\Omega^{\pm}(n, q)$. *Let* $G \leqslant \Gamma L(n, q)$, $\Gamma\mathrm{Sp}(n, q)$, $\Gamma U(n, q)$ *resp.* $\Gamma O^{\pm}(n, q)$, *and let* $K \leqslant G$ *with* $K \ngeqslant G^\natural$. *Assume that* G *induces a primitive rank* r *permutation group on the set of cosets of* K *in* G. *If* K *is not the stabilizer of a proper subspace (other than the radical if* $G^\natural = \Omega(2m+1, q)$ *with* q *even), then* $r > n/16$. *(Moreover,* $r > n/4$ *when* $G^\natural$ *is* $\mathrm{SL}(n, q)$, *and* $r \geqslant n/8$ *when* $G^\natural$ *is* $\mathrm{Sp}(n, q)$ *or* $\mathrm{SU}(n, q)$*).*

The analogues of Theorem 3 for S_n and A_n are due to Bannai [1, pp. 477–478], and deducing it from Theorems 1 and 2 follows his approach. Theorem 3 should be compared with Seitz's result [33]: given r and l, for all large q every rank r permutation representation of a rank l Chevalley (or twisted) group is essentially known. Combining these results yields the following curious consequence.

COROLLARY. *For each integer* $r \geqslant 2$ *there are only finitely many presently known finite simple groups possessing presently unknown primitive rank* r *permutation representations.*

This corollary was conjectured in 1973 by Peter M. Neumann. It implies, for example, that the enumerations for $r = 2$ and 3 in [6] and [21] were finite problems, a fact of which those authors were not aware. However, the corollary is not very effective. For example, if $r = 4$ and $G = \Omega^{\pm}(n, q)$ then necessarily $n \leqslant 63$ and $q \leqslant 1 + 4\{4(2^{31}31!)^{1/2} + 3(2^{31}31!)^{3/2}\}$ (cf. Section 5).

As in Patton [29], the proofs of Theorems 1 and 2 require some knowledge of the first cohomology groups of classical groups acting on their natural modules. The cases $\mathrm{SL}(n, q)$ and $\mathrm{Sp}(n, q)$ require, in addition, little more than McLaughlin's beautiful results [23; 24]; while $\mathrm{SU}(n, q)$ and especially $\Omega^{\pm}(n, q)$ involve the less pleasant [20]. All cases use induction, based upon the action of the centralizer $C_G(x)$ of a suitable type of 1-space x on $O_p(C_G(x))$ (where p will always denote the prime dividing q).

Finally, it should be noted that, in Theorems 2 and 3, $\mathrm{Sp}(2m, q)$ is not excluded when q is even. Instead, we have used the isomorphism $\mathrm{Sp}(2m, q) \cong \Omega(2m + 1, q)$ in order to include the cases $K \trianglerighteq \Omega^{\pm}(2m, q)$. Also, in Theorem 2 the only time $|G : K|$ actually equals q^θ is when $G^\natural = \mathrm{Sp}(4, 3)$.

I am grateful to Peter M. Neumann for several helpful suggestions concerning this paper, especially as regards the history of Galois' theorem.

2. Preliminaries

Our notation for the classical groups is reasonably standard. Transvections are familiar; the less familiar long root elements of orthogonal groups are discussed in [20, Sects. 3, 4]. The underlying vector space will always be denoted by V. If $S \leqslant G$ and W is an S-invariant subspace, then $C_S(W)$ is the subgroup of S inducing the identity on W and $C_W(S)$ is the set of vectors fixed by S, while $S^W = S/C_S(W)$ and $[W, S] = \langle w^s - w \mid w \in W,\ s \in S\rangle$; the corresponding notation will also be used when W is merely an S-invariant section of V.

We will need a cohomological property of the following groups:

(*) $\mathrm{SL}(2, q)$, $q > 3$ odd; $\mathrm{SL}(3, q)$, $q > 2$; $\mathrm{SL}(4, q)$, $q = 2$; $\mathrm{Sp}(4, q)$, q odd; $\mathrm{SU}(5, q)$; $\mathrm{SL}(2, 5)$, regarded as inside $\mathrm{SL}(2, q) = \mathrm{SL}(2, 9)$.

Lemma 0. (i) *Suppose that $S \leqslant G = \mathrm{GL}(V)$, that $S = S'$ and that H is an S-invariant hyperplane such that $H = [H, S] \oplus C_H(S)$. If $S^{[H,S]}$ is one of the groups (*) in its natural representation (or the representation contragredient to the natural one), then $V = [H, S] \oplus C_V(S_0)$ for some $S_0 \leqslant S$ with $S_0^{[H,S]} = S^{[H,S]}$.*

(ii) *Let $S \leqslant G = \Omega^{\pm}(V)$, assume that S fixes the singular point x, and set $\bar V = x^\perp/x$. Suppose that $\bar V = [\bar V, S] \perp [\bar V, S]^\perp$ and $[\bar V, S] = \bar V_1 \oplus \bar V_2$ with each $\bar V_i$ totally singular and $S^{\bar V_1}$ as in (*). Then $V = [V, S_0] \perp C_V(S_0)$ for some $S_0 \leqslant S$ such that $S_0^{[\bar V,S]} \cong S^{[V,S]}$ and the S_0-modules $[V, S_0]$ and $[\bar V, S_0]$ are isomorphic.*

Proof. (i) The group $Q = C_G(H) \cap C_G(V/H)$ consists of all transvections with axis H. Since $S = S'$ it centralizes V/H, and hence acts the same on Q as on H. (If $v \in V - H$ then $t \to v^t - v$, $t \in Q$, defines an S-isomorphism.) Since $S = S'$ and S also centralizes $H/[H, S]$, it centralizes $V/[H, S]$, so that $Q \cap S$ consists of transvections with directions in $[H, S]$. Thus, $Q \cap S \leqslant [Q, S]$. The irreducibility of S on $[Q, S]$ then implies that $Q \cap S$ is 1 or $[Q, S]$.

Suppose that $Q \cap S = [Q, S]$. Then both S and $Q \cap S$ act transitively on $[H, S] + v$ for any $v \in V - H$, so $S = (Q \cap S)\, C_S(v)$. We may thus replace S by $C_S(v)$ and reduce to the case $Q \cap S = 1$, $S \cong S^H$.

By results of Higman [16] and McLaughlin [25] (cf. [21, Sec. 2] and further, references given there), $H^1(S, [Q, S]) = 0$. Thus, $\mathrm{Ext}_{GF(q)S}(GF(q), [H, S]) = 0$ and V must decompose as required.

(ii) Let $\bar{V}_i = V_i/x$. By the dual of (i), we may assume that $\bar{V}_i = [\bar{V}_i, S] \oplus x$. Then $[V, S] = [V_1 + V_2, S] = [V_1, S] \oplus [V_2, S]$ behaves as desired.

Remark. The following more elementary argument applies when $Z(S^H) \neq 1$ or $Z(S^{\bar{V}}) \neq 1$, respectively. By the Frattini argument, we may assume that $Z = Z(S) \neq 1$. Then $V = [V, Z] \oplus C_V(Z)$ with each summand S-invariant. Since S is generated by its p'-elements, it follows easily that $[V, Z] = [V, S]$ is S-isomorphic to $[H, S]$ resp. $[\bar{V}, S]$ and that $C_V(Z) = C_V(S)$, as required.

3. Proof of Theorem 1

Define α as follows.

q	odd, $q \neq 3$	3, or even but $q \neq 2$	2
α	0	1	2

We will prove inductively that, in addition to (i) or (ii) holding, K contains a subgroup $S \simeq \mathrm{SL}(2 + \alpha, q)$ (or $\mathrm{SL}(2, 5)$ if $q = 9$) such that $V = [V, S] \oplus C_V(S)$ with $\dim[V, S] = 2 + \alpha$; in particular, S contains nontrivial transvections.

If $n = 3$ this follows from Dickson [7, Ch. 12], Mitchell [26] and Hartley [13], so suppose that $n \geqslant 4$ (and $n \geqslant 5$ if $q = 2$). Let H be any hyperplane, $P = C_G(V/H)$, and $Q = C_P(H)$. Then $|Q| = q^{n-1}$ and Q consists of transvections.

Lemma 1. *If* $|K \cap Q| \leqslant q^\alpha$ *then* $|P^H : (K \cap P)^H| \leqslant q^{(n-\alpha-1)(n-\alpha-2)/2}$.

Proof. By hypothesis,

$$\begin{aligned} q^{(n-\alpha)(n-\alpha-1)/2} &\geqslant |G : K| \geqslant |P : K \cap P| \\ &= |P : (K \cap P)Q|\,|(K \cap P)Q : K \cap P| \\ &= |P^H : (K \cap P)^H|\,|Q : K \cap Q| \geqslant |P^H : (K \cap P)^H|\, q^{n-1-\alpha}, \end{aligned}$$

so the lemma follows using arithmetic.

Lemma 2. *If* $|K \cap Q| \leqslant q^\alpha$ *(for some hyperplane* H*), then* $K \cap P$ *contains a subgroup* S *of one of the required types.*

Proof. By Lemma 1 and induction, $(K \cap P)^H$ has such a subgroup. Hence, by Lemma 0, so does $K \cap P$.

LEMMA 3. *If* $|K \cap P| > q^\alpha$ *for every hyperplane* H, *then* K *contains a subgroup* S *of one of the required types.*

Proof. Let W be an irreducible K-subspace. Then $W \cap H$ is the axis of more than q^α transvections of W lying in K for each hyperplane $H \not\supseteq W$. Thus, $d = \dim W > 1$ and K induces at least $\mathrm{SL}(d, q)$ or $\mathrm{Sp}(d, q)$ on W (e.g., [30, 31, 34, 20]); moreover, if $\alpha \geqslant 1$ then only $\mathrm{SL}(d, q)$ is possible, while if $\alpha = 2$ then $d \geqslant 4$. It follows that K has a subgroup S such that $S = S'$ and S is generated by transvections, while $S^W \cong \mathrm{SL}(2 + \alpha, q)$ or $\mathrm{SL}(2, 5)$ and $[W, S]$ is the natural module for S^W. Since S centralizes $V/[W, S]$, repeated use of Lemma 0 produces the desired subgroup of K.

Completion of the proof. We have obtained the desired S. Let K^* denote the subgroup generated by all transvections in K.

We may assume that K is irreducible. Then $V = V_1 \oplus \cdots \oplus V_k$ for irreducible K^*-subspaces V_i permuted transitively by K.

If $k = 1$ then K^* is $\mathrm{SL}(n, q)$, $\mathrm{Sp}(n, q)$, $O^{\pm}(n, 2)$, S_{n+1}, S_{n+2}; or possibly $\mathrm{SL}(n, 3)$, $\mathrm{Sp}(n, 3)$ or $\mathrm{SU}(n, 3)$ when $q = 9$ (McLaughlin [23, 24] if $q \neq 9$; Piper [30, 31] and Wagner [34] if $q = 9$). Only in the first two cases is $|G : N_G(K^*)| \leqslant q^{n(n-1)/2}$.

If $k > 1$ then $K \leqslant \Gamma L(n/k, q) \wr S_k$, so $|G : K| > q^{n(n-1)/2}$. Thus, (ii) must hold if (i) does not, and the theorem is proved.

4. PROOF OF THEOREM 2

Let $\alpha = 0$ for $G^\natural = \mathrm{Sp}(2m, q)$ (with q odd) or $\mathrm{SU}(n, q)$; and define α as in Section 3 for the orthogonal groups. Define β as follows.

$G^\natural$	$\mathrm{Sp}(2m, q)$, q odd	$\mathrm{SU}(n, q)$	$\Omega^+(2m, q)$	$\Omega^-(2m, q)$	$\Omega(2m + 1, q)$
β	m	$n - 1$	$m - 1 - \alpha$	$m - 2 - \alpha$	$m - 1 - \alpha$

We must prove that, if $|G : K| < q^{\beta(\beta+1)/2}$ (or if $|G : K| < q^{[n^2/4]}$ in the unitary case), then K is reducible. This time our inductive hypothesis is that K also has a subgroup S satisfying the following conditions: (a) $V = [V, S] \perp C_V(S)$ with $[V, S]$ nonsingular; (b) if V is symplectic (with q odd) or unitary, then $S \cong \mathrm{Sp}(4, q)$ resp. $\mathrm{SU}(5, q)$, $\dim[V, S] = 4$ resp. 5, and S acts naturally on $[V, S]$; (c) if V is orthogonal then $S \cong \mathrm{SL}(2 + \alpha, q)$ (or $\mathrm{SL}(2, 5)$ if $q = 9$), $\dim[V, S] = 2(2 + \alpha)$, and S fixes two complementary totally singular subspaces of $[V, S]$, on one of which it acts as in (*). Note that in each case S contains nontrivial elements of (long) root groups of G.

If $n = \dim V \leqslant 6$ in (b), or $n \leqslant 8$ in (c), then all of this holds by Cooperstein [5]. Thus, suppose that $n > 6$ or 8, respectively.

Let x be a totally isotropic (or totally singular) point, $P = C_{G^\natural}(x)$ and $Q = C_P(x^\perp/x)$. Then P/Q is $\mathrm{Sp}(2m-2, q)$, $\mathrm{SU}(n-2, q)$ or $\Omega^\pm(n-2, q)$, and acts on $Q/Z(Q)$ as it does on its standard module $x^\perp/x$; moreover, if $Z(Q) \neq 1$, then V is symplectic (with q odd) or unitary, $Z(Q) = Q'$ consists of q transvections, Q is a special group of order $q^{2\beta-1}$, and commutation induces a nondegenerate alternating $\mathrm{GF}(q)$-bilinear form on $Q/Z(Q)$ preserved by P/Q (cf. [6, Sect. 3]).

The first two lemmas are proved exactly as before.

Lemma 1′. *If* $|Q : K \cap Q| \geqslant q^\beta$ *then* $|P^{x^\perp/x} : (K \cap P)^{x^\perp/x}|$ *is less than* $q^{\beta(\beta-1)/2}$ *(or* $q^{[(n-2)^2/4]}$ *in the unitary case).*

Lemma 2′ *If* $|Q : K \cap Q| \geqslant q^\beta$ *for some* x*, then* $K \cap P$ *contains a subgroup* S *of one of the required types.*

The third lemma is somewhat harder, at least in the orthogonal case:

Lemma 3′. *If* $|Q : K \cap Q| < q^\beta$ *for every* x*, then* K *contains a subgroup of one of the required types.*

Proof. We first show that each $K \cap Q$ contains subgroups of order greater than q^α consisting entirely of long root elements. This requires considering the individual cases separately. If $G^\natural = \Omega^+(2m, q)$ or $\Omega(2m+1, q)$, then Q has a subgroup R of order q^{m-1} consisting of long root elements (corresponding to a totally singular $m-1$-space of $x^\perp/x$ as in [6, (3.1)]), and $|R| \cdot |K \cap Q| > q^\alpha |Q|$ by hypothesis; if $G = \Omega^-(2m, q)$, there is such a subgroup R of order q^{m-2}. In either case, $|Q|\,|K \cap R| \geqslant |R(K \cap Q)|\,|K \cap R| = |R|\,|K \cap Q| > q^\alpha |Q|$. If $G^\natural$ is $\mathrm{Sp}(2m, q)$ (with q odd) or $\mathrm{SU}(n, q)$ then we must only show that $K \cap Z(Q) \neq 1$. So suppose that $K \cap Z(Q) = 1$. Then $(K \cap Q)\,Z(Q)/Z(Q)$ consists of pairwise perpendicular vectors in a $2\beta - 2$-dimensional symplectic geometry, and hence has order at most $q^{\beta-1}$. Consequently, $|K \cap Q| \leqslant q^{\beta-1}$ and $|Q : K \cap Q| \geqslant q^\beta$, contrary to our hypothesis.

If $G^\natural$ is symplectic or unitary, it follows that $K \geqslant G^\natural$, and the lemma is clear.

Suppose that $G^\natural$ is orthogonal, and let K^* be the group generated by all long root elements of K. If K^* is irreducible, then $K^* = G^\natural$ by [20]. So suppose further that W is a K^*-invariant subspace minimal with respect to having $W \supset \mathrm{rad}\, V$.

Pick any point $x \notin W^\perp$ and a long root element $t \neq 1$ in $K \cap Q$. Set $A(t) = [V, t]$. Then $A(t)$ is a 2-dimensional totally singular subspace, and $C_V(t) = A(t)^\perp$. Since $W^t = W \not\subset A(t)^\perp$, necessarily $A(t) \cap \mathrm{rad}\, W \neq 0$. In particular, since $\mathrm{rad}\, W$ is invariant under K^* we must have $W = \mathrm{rad}\, W$. Set $W^* = W/\mathrm{rad}\, V$.

Now $A(t) \not\subset W^\perp$ implies that t induces a transvection on W with axis $A(t)^\perp \cap W$. Each hyperplane of W containing $\mathrm{rad}\, V$ occurs as $x_1{}^\perp \cap W$ for some point x_1; and if $t_1 \in C_K(x_1) \cap C_K(x_1{}^\perp/x_1)$ is a nontrivial long root element then $A(t_1)^\perp \cap W$ can only be $x_1{}^\perp \cap W$. Consequently, each hyperplane of W^* is the axis of more than q^α transvections. Then K^{*W^*} is $\mathrm{SL}(W^*)$, $\mathrm{Sp}(W^*)$ or $\mathrm{SL}(2, 5) < \mathrm{SL}(2, 9) = \mathrm{SL}(W^*)$. In any event, $2 + \alpha$ suitably chosen root elements of K^* will generate the S required in the lemma.

The proof of Theorem 2 can now be completed by imitating the argument at the end of Section 3, this time using [20] in the orthogonal and unitary cases.

5. Proof of Theorem 3

We will only consider the case $G^\natural = \mathrm{SL}(n, q)$, $q > 2$, the remaining cases being quite similar. We may assume that $n \geqslant 3$.

For each $g \in G - Z(G)$, $|G : K| \leqslant 2 |G : C_G(g)|^{r-1}$ (see Bannai [1, pp. 475–477]). Let $g \neq 1$ be a transvection. If K is irreducible then Theorem 1 yields

$$q^{\frac{1}{2}(n-1)(n-2)} < |G : K| \leqslant 2 \left\{\frac{q^n - 1}{q - 1} \frac{q^{n-1} - 1}{q - 1} (q - 1)\right\}^{r-1} < qq^{r-1}q^{2(n-1)(r-1)},$$

so that $n - 4 < 4(r - 1)$.

It should be noted that the orthogonal group estimates are improved by a factor of 2 if $O^\pm(n, q)$ is used instead of $\Omega^\pm(n, q)$. For then, g may be taken to be a reflection or a transvection.

Also, the same proof handles the case in which $G/Z(G)$ contains graph automorphisms as well as diagonal or field automorphisms of $G^\natural/Z(G^\natural)$.

6. Remarks on Seitz's Theorem

Assume that G is as in Theorem 3. Let W be its Weyl group and $B = UH$ a Borel subgroup, where U is a Sylow p-subgroup of G and H is assumed abelian. Seitz [33] proved that $q \leqslant 5(1.8)^{l(r,w)}$, where $l(r, w) = r\,|W|^{1/2} + (r - 1)\,|W|^{3/2}$. (Actually, he used $l(r, w) = r\,|W| + (r - 1)\,|W|^2$, but this slight improvement is implicit in his proof.) In this section we will show that $q \leqslant 4l(r, W) + 1$.

The proof of [33, Theorem 2] shows that U has at most $l(r, W)$ orbits on the set of cosets of K in G.

Following [33], we will prove by induction on $|W|$ that, if $K \leqslant G$ and U has at most l orbits on the set Ω of cosets of K in G for some integer $l < (q - 1)/4$, then K contains (the center of) a long root group of G (merely a root group for the cases $\Omega^\pm(2m, q)$, $\Omega(3, q)$ and $\Omega^-(4, q)$).

If $|W| = 2$ it is straightforward to use Dickson [7, Ch. 12], Mitchell [26] and Hartley [13] to check the above assertion. We will thus suppose that $|W| > 2$.

Let P and Q be as in Sections 3 and 4, chosen so that $P \geqslant U$ and H normalizes

P. Write $P = QR$, where R is the centralizer of a nonsingular 2-space (or the stabilizer in P of a non-incident point-hyperplane pair in the $\mathrm{SL}(n, q)$ case). Let $K = G_\alpha$, $\alpha \in \Omega$. Since RH acts on the set of Q-orbits on α^{PH}, induction produces a root group X_s of R of the desired length fixing some $\beta^Q \subseteq \alpha^{PH}$; moreover, we can choose X_s so that $QX_s \trianglelefteq U$. (Here, s is a root in the root system Δ on which W acts.)

Clearly, H acts transitively on the set of U-orbits in β^{UH}; if H_0 is the stabilizer of β^U, then $|H : H_0| \leqslant l < (q-1)/4$ and H_0 fixes some $\gamma = \beta\bar{q} \in \beta^U$, $u \in U$. Then $QX_s = QX_s\bar{q} = Q(QX_s)_\gamma$. Since $H_0 \leqslant G_\gamma$, it acts on $(QX_s)_\gamma$, so Lemma 3 of Seitz [33] implies that $(QX_s)_\gamma$ is a product of root groups which correspond to Δ. Since $Q(QX_s)_\gamma/Q \cong X_s$, we deduce that $(QX_s)_\gamma \geqslant X_s$.

This completes the inductive proof whenever s is automatically not a short root, and hence in all cases except $G'' = \Omega(5, q)$ or $\Omega^-(6, q)$. But for these cases we simply reverse the Dynkin diagram, apply the result proved for $\mathrm{Sp}(4, q)$ and $\mathrm{SU}(4, q)$, and obtain the desired long root group of $\Omega(5, q)$ or $\Omega^-(6, q)$.

Consequently, back in the situation on Theorem 3 we find that if $q > 4l(r, W) + 1$, then K contains a (long) root group. By [23, 24, 20], all irreducible possibilities for K are known. None produces a value of r permitted by the inequality $q > 4l(r, W) + 1$.

Remarks. 1. If H is nonabelian, then $q \leqslant 4l(br, W) + 1$, where $q = p^b$.

2. It would obviously be desirable to have much better bounds on q (such as, perhaps, $q \leqslant 16r$).

3. Only the BN structure of the classical groups was needed in the inductive step. Thus, when all those subgroups K of the exceptional Chevalley groups have been classified which satisfy $O_p(K) < Z(K)$ and are generated by a class of long root elements, then an improved bound such as $q \leqslant 4l(r, W) + 1$ will again hold. (Similar statements can clearly also be made concerning analogues of Theorems 2 and 3.)

4. Seitz's proof depends only on the number r_0 of irreducible constituents common to the permutation characters $1_B{}^G$ and $1_K{}^G$, counting multiplicities. Our Theorem 3 depends on the rank r itself. In view of [21, Theorems I' and II'], it seems reasonable to expect that an analogue of Theorem 3 exists with r_0 in place of r.

7. Further Variations

The bounds in Theorem 2 are much poorer than those in Theorem 1. This is due to the possibility that $K \cap Q \neq 1$ (and even that $|K \cap Q|$ is a large power of q). One way to improve these bounds would be to determine the irreducible groups meeting some Q nontrivially; this seems particularly feasible in the orthogonal groups.

However, even then the cohomological obstacles caused by $SL(2, 3)$ and $SL(2, 2^i)$ would still remain. It is not clear how to handle these; but then they do in part produce interesting examples. For example, they are involved in subgroups of the indicated small indices in the following groups: $Sp(4, 3)$ and $\Omega(5, 3)$, 3^3 and $3^2 \cdot 5$; $SU(4, 2)$ and $\Omega^-(6, 2)$, $2^3 \cdot 5$; $SL(4, 2)$ and $\Omega^+(6, 2)$, 2^3; $SU(4, 3)$, $2 \cdot 3^4$; and $SU(6, 2)$, $2^6 \cdot 33$.

It seems that the best results of this type should at least deal with the case $|G : K| \leqslant |G : B|$. Arithmetic prevented this in the proof of Lemma 1. For $G^\natural = SL(n, q)$ and large odd q this inequality can in fact be proved. Namely, in both Theorems 1 and 2, all estimates $|G : K| < q^\theta$ (say) can be replaced by $|G : K| < cq^\theta$ for a constant c chosen so that induction will apply. If $G^\natural = SL(n, q)$, the proof of Theorem 1 can be suitably modified when $c = 12/11$ (some care must be taken since S need not exist). For fixed n and sufficiently large odd q, this handles the case $|G : K| \leqslant |G : B| < (12/11)q^{1/2n(n-1)}$. However, this seems to be an unsatisfactory method for improving the bounds obtained earlier. What is needed is a different approach, perhaps one employing properties of the characters and centralizer algebra of the permutation representation on the cosets of K.

8. Historical Remarks

Galois' theorem that $|PSL(2, q) : K| \geqslant q + 1$ if and only if the prime $q \neq 2, 3, 5, 7, 11$ was stated in his famous letter to Auguste Chevalier [11, pp. 411–412]. Part of a proof is given at the end of his second memoir [11, pp. 443–444]. In particular, exceptions are described for $q = 5$, 7 and 11.

The first published proof that no exceptions occur for prime $q > 11$ is due to Jordan [17] (reproduced in [19, pp. 666–667]). Analytic proofs of the existence of exceptions were given by Betti [2, 15] and Hermite [14, 15]. Much later, in 1881 Gierster [12] gave a different proof of Galois' theorem by enumerating all the subgroups of $PSL(2, q)$ for odd prime q. Further references and historical remarks (as well as applications to the modular equation) can be found in [10, I. 1, pp. 215–221, 513–514, 533, 547; II. 2, pp. 239–240, 315, 390–391, 429–431].

According to Loewy [22], the analogue of Galois' theorem for prime power q was proved by Moore in 1894 and the result communicated to Fricke. The first published proof for arbitrary q was obtained by a complete enumeration of the subgroups of $PSL(2, q)$; this was accomplished by Burnside [3] (for q even), Wiman [35] and Moore [28]. Moore's enumeration was completed in 1898, and presented to the American Mathematical Society; the abstract [28] of his talk indicates the subgroups and explicitly states the generalization of Galois' theorem. His paper was submitted to *Mathematische Annalen* (cf. Dickson [7, footnotes on pp. 49 and 260]), but was withdrawn and published after Wiman's paper [35] of 1899 (cf. Loewy [22]). Of course, the standard reference for this enumeration has become Dickson [7, Ch. 12]. It should, however, be noted that Dickson was not the first to determine the subgroups of PSL(2, q) of order divisible by the prime dividing q.

In 1870, Jordan[18; 19, pp. 666–667] made the natural conjecture concerning Sp($2m$, q) for $m \geqslant 2$ and q an odd prime, but was only able to deal with Sp(4, 3) and Sp(4, 5). Dickson [9] later handled Sp(4, q) for all prime q, without enumerating all subgroups. The general case of Sp(4, q) with q odd was settled by Mitchell [27], this time by a complete enumeration.

The groups PSL(3, q) were considered by Burnside [4] for very special primes q; for arbitrary primes q, Dickson [8] enumerated all subgroups of order divisible by q, using an explicit knowledge of all conjugacy classes of q-groups. All subgroups of PSL(3, q) and PSU(3, q) were found by Mitchell [26] for odd q and his student Hartley [13] for even q; only then was information available concerning the size of $|G : K|$.

References

1. E. Bannai, Maximal subgroups of low rank of finite symmetric and alternating groups, *J. Fac. Sci. Univ. Tokyo Sect. I* **18** (1971/72), 475–486.
2. E. Betti, Sopra l'abassamento dell'equazioni modulari, *Ann. Fis. Mat.* **4** (1853), 90.
3. W. Burnside, On a class of groups defined by congruences, *Proc. London Math. Soc.* **25** (1894), 113–139.
4. W. Burnside, On a class of groups defined by congruences, *Proc. London Math. Soc.* **26** (1895), 58–106.
5. B. N. Cooperstein, Minimal degree for a permutation representation of a classical group, *Israel J. Math.* **30** (1978), 213–235.
6. C. W. Curtis, W. M. Kantor, and G. M. Seitz, The 2-transitive permutation representations of the finite Chevalley groups, *Trans. Amer. Math. Soc.* **218** (1976), 1–57.
7. L. E. Dickson, "Linear Groups, with an Exposition of the Galois Field Theory," 1900; reprinted, Dover, New York, 1958.
8. L. E. Dickson, Determination of the ternary modular linear group, *Amer. J. Math.* **27** (1905), 189–202.
9. L. E. Dickson, The minimum degree τ of resolvents for the p-section of the periods of hyperelliptic functions of four periods, *Trans. Amer. Math. Soc.* **6** (1905), 48–57.
10. "Encycklopädie der Mathematischen Wissenschaften," Teubner, Leipzig, 1898–1921.
11. E. Galois, Œuvres mathématiques, *J. de Math.* **11** (1846), 381–444.
12. J. Gierster, Die Untergruppen der Galois'schen Gruppe der Modulargleichungen für den Fall eine primzahligen Transformationsgrades, *Math. Ann.* **18** (1881), 319–365.
13. R. W. Hartley, Determination of the ternary linear collineation groups whose coefficients lie in the $GF(2^n)$, *Ann. of Math.* **27** (1926), 140–158.
14. C. Hermite, Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres, *J. Reine Angew. Math.* **40** (1850), 279–290.
15. C. Hermite, Sur la théorie des équations modulaires, *C. R. Acad. Sci. Paris* **49** (1859), 110–118.

16. D. G. Higman, Flag-transitive collineation groups of finite projective spaces, *Illinois J. Math.* **6** (1962), 434–446.
17. C. Jordan, Note sur les équations modulaires, *C. R. Acad. Sci. Paris* **66** (1868), 308–312.
18. C. Jordan, Sur la division des functions hyperelliptiques, *C. R. Acad. Sci. Paris* **70** (1870), 1028–1032.
19. C. Jordan, "Traité des Substitutions et des Équations Algébriques," Gauthier–Villars, Paris, 1870.
20. W. M. Kantor, Subgroups of classical groups generated by long root elements, *Trans. Amer. Math. Soc.* **248** (1979), 347–379.
21. W. M. Kantor and R. A. Liebler, The rank 3 permutation representations of the finite classical groups, submitted.
22. A. Loewy, Review of [28], *J. Fortschr. Math.* **34** (1905), 172–173.
23. J. McLaughlin, Some groups generated by transvections, *Arch. Math.* **18** (1967), 364–368.
24. J. McLaughlin, Some subgroups of $SL_n(F_2)$, *Illinois J. Math.* **13** (1969), 108–115.
25. J. McLaughlin, unpublished.
26. H. H. Mitchell, Determination of the ordinary and modular ternary linear groups, *Trans. Amer. Math. Soc.* **12** (1911), 207–242.
27. H. H. Mitchell, The subgroups of the quaternary abelian linear groups, *Trans. Amer. Math. Soc.* **15** (1914), 379–396.
28. E. H. Moore, The subgroups of the generalized finite modular group, Decennial Publications of the Univ. of Chicago **9** (1904), 141–190. Abstract in *Bull. Amer. Math. Soc.* **5** (1898), 3, 7–8.
29. W. H. Patton, "The Minimum Index for Subgroups in Some Classical Groups: A Generalization of a Theorem of Galois," Ph. D. thesis, University of Illinois at Chicago Circle, 1972.
30. F. C. Piper, On elations of finite projective spaces of odd order, *J. London Math. Soc.* **41** (1966), 641–648.
31. F. C. Piper, On elations of finite projective spaces of even order, *J. London Math. Soc.* **43** (1968), 459–464.
32. H. Pollatsek, unpublished.
33. G. M. Seitz, Small rank permutation representations of finite Chevalley groups, *J. Algebra* **28** (1974), 508–517.
34. A. Wagner, Groups generated by elations, *Abh. Math. Sem. Univ. Hamburg* **41** (1974), 190–205.
35. A. Wiman, Bestimmung alle Untergruppen einer doppelt unendlichen Reihe von einfachen Gruppen, *Bihang till K. Svenska Vet.-Akad. Handl.* **25** (1899), 1–47.